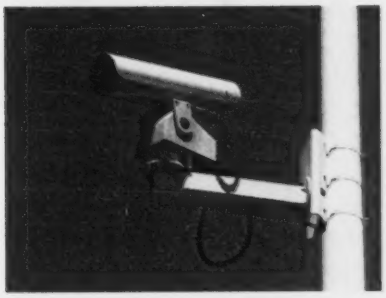
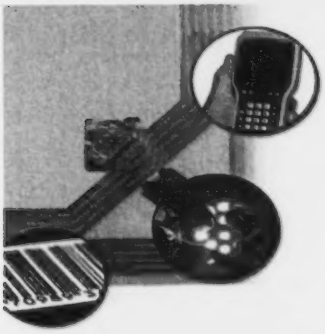
Office of the Privacy Commissioner of Canada



2010-2011

Report on Plans and Priorities



The original version was signed by

The Honourable Robert D. Nicholson, P.C., Q.C., M.P.
Minister of Justice and Attorney General of Canada

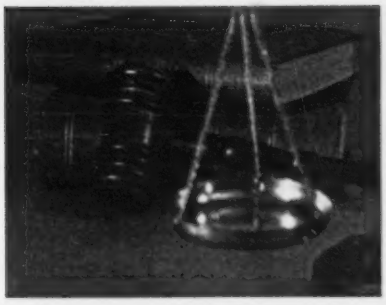


Table of Contents

Message from the Privacy Commissioner of Canada 1

Section I: Overview 3

1.1 Summary Information 3
1.2 Planning Summary 4

Section II: Analysis of Program Activities 11

2.1 Strategic Outcome 11
2.2 Program Activity 1: Compliance Activities 12
2.3 Program Activity 2: Research and Policy Development 15
2.4 Program Activity 3: Public Outreach 17
2.5 Program Activity 4: Internal Services 20

Section III: Supplementary Information 22

3.1 List of Tables 22
3.2 Other Items of Interest 22

Message from the Privacy Commissioner of Canada

I am pleased to present this 2010-2011 *Report on Plans and Priorities*, which sets out the strategic directions, priorities, expected results and spending estimates for the Office of the Privacy Commissioner of Canada (OPC) for the coming fiscal year.

At the start of this final year of my seven-year term as Privacy Commissioner, I am reflecting on both the challenge and the sense of satisfaction that have come from guiding this Office through a period of significant tumult and into an era of unprecedented growth, relevance and dynamism.

The vitality of today's OPC was driven home last summer when we published our investigative report on the privacy policies and practices of social networking giant Facebook. As the world lavished attention on our work, it was clear how much privacy continues to matter, and that our organization has a powerful role to play in securing the privacy rights of Canadians.

As this *Report on Plans and Priorities* makes clear, we are carrying out our mandate in several important ways: through our inquiries and complaints investigations functions, our audits and Privacy Impact Assessment reviews, our communications and strategic outreach efforts, and our legal, Parliamentary and policy-review work. We are also investing efforts in engaging the international community, because data flows respect no borders.

In the coming year, I am confident that still greater things lie ahead for this organization. We are finding ways to concentrate our efforts where they will yield the most impact. Toward that end, we have selected what we consider to be the four most significant emerging challenges to the privacy rights of Canadians: information technology, national security, the protection of identity, and genetic information. We are also reengineering our investigative processes in order to focus on systemic issues, and to wipe out what was, not long ago, a crippling backlog of cases.

Over the past few years, the Office of the Privacy Commissioner of Canada has matured into a stable and sophisticated organization with talented employees dedicated to serving the public. As a credible and influential voice for the protection of privacy, our commitment in the year ahead is to maintain this momentum with a bold, focused and forward-looking agenda.

The OPC's five corporate priorities for 2010-2011 are to:

- redefine service delivery through innovation to maximize results;
- provide leadership to advance four priority privacy issues (information technology, national security, identity integrity and protection, genetic information);
- strategically advance global privacy protection for Canadians;
- support Canadians, organizations and institutions to make informed privacy decisions, and
- enhance and sustain organizational capacity.

I am pleased to be able to lead this Office through the final year of my mandate, and look forward to the opportunity to report on more successes as the year unfolds.

The original version was signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Section I: Overview

1.1 Summary Information

Raison d'être

The mandate of the Office of the Privacy Commissioner of Canada is to oversee compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's private-sector privacy law. The mission of the Office is to protect and promote the privacy rights of individuals[1].

Responsibilities

The Privacy Commissioner of Canada, Jennifer Stoddart, is an Officer of Parliament who reports directly to the House of Commons and the Senate. The Commissioner is an advocate for the privacy rights of Canadians and her powers include:

- investigating complaints, conducting audits and pursuing court action under two federal laws;
- publicly reporting on the personal information-handling practices of public- and private-sector organizations;
- supporting, undertaking and publishing research into privacy issues, and
- promoting public awareness and understanding of privacy issues.

The Commissioner works independently from other parts of the government to investigate complaints from individuals with respect to the federal public sector and the private sector. The focus is on resolving complaints through negotiation and persuasion, using mediation and conciliation as appropriate. If voluntary co-operation is not forthcoming, however, the Commissioner has the power to summon witnesses, administer oaths, and compel the production of evidence. In cases that remain unresolved, particularly under PIPEDA, the Commissioner may seek an order from the Federal Court to rectify the situation.

Strategic Outcome and Program Activity Architecture (PAA)

In line with its mandate, the OPC pursues as its Strategic Outcome the protection of the privacy rights of individuals. Toward that end, the Office's architecture of program activities is composed of three operational activities and one management activity. The PAA diagram below presents information at the program activity level:

<table>
<tr><td>Strategic Outcome</td><td colspan="3">The privacy rights of individuals are protected.</td></tr>
<tr><td rowspan="2">Program Activity</td><td>1. Compliance Activities</td><td>2. Research and Policy Development</td><td>3. Public Outreach</td></tr>
<tr><td colspan="3">4. Internal Services</td></tr>
</table>

[1] Reference is made to "individuals" in accordance with the legislation.

Alignment of PAA to Government of Canada Outcomes

Federal departments are required to report on how their PAA aligns with the Government of Canada Outcomes. The Privacy Commissioner, being independent from government, reports directly to Parliament. The Strategic Outcome and the expected results from the work of the Office of the Privacy Commissioner of Canada are detailed in Section II of this *Report on Plans and Priorities*.

1.2 Planning Summary

The following two tables summarize the total planned financial and human resources required by the OPC over the next three fiscal years.

Financial Resources ($000)

	2010-2011	2011-2012	2012-2013
Planned Spending	**22,390**	**22,413**	**22,413**
Adjustment:			
*Electronic Commerce Protection Act (ECPA)***	849	2,154	2,154
Adjusted Planned Spending	**23,239**	**24,567**	**24,567**

Human Resources (FTEs**)

	2010-2011	2011-2012	2012-2013
Planned FTEs	**173**	**173**	**173**
Adjustment:			
*Electronic Commerce Protection Act (ECPA)****	4	6	6
Adjusted Planned FTEs	**177**	**179**	**179**

** FTE: Full-Time Equivalent.
***: Pending final Parliamentary and Treasury Board approvals.

Contribution of Priorities to the Strategic Outcome

The OPC has a single Strategic Outcome (SO 1), which is that the privacy rights of individuals be protected. Toward that end, the OPC identified five corporate priorities: four are operational in nature and the fifth relates to the management of the organization.

The table below describes how each corporate priority contributes to the Strategic Outcome, and what the OPC plans to do in 2010-2011 to make progress toward each priority. More detail about those planned activities is provided in Section II.

Corporate Priority	Type[2]	Link to Strategic Outcome	Description
1. Redefine service delivery through innovation to maximize results	New	SO 1	Effective delivery of complaint-resolution processes is essential to the protection of individual privacy rights. The OPC will: • Adapt its processes to be more strategic and proactive while reflecting Canadians' needs and expectations on privacy remedies. • Explore collaborative opportunities, including enforcement measures, with provincial/territorial and international counterparts.
2. Provide leadership to advance four priority privacy issues (information technology, national security, identity integrity and protection, and genetic information)	Previous	SO 1	In 2008-2009, the OPC launched a horizontal approach to focus on four emerging privacy issues over the next few years. A strategic plan for each priority issue sets goals and identifies concrete action items. More details are available on the OPC website at http://www.priv.gc.ca/aboutUs/message_e.cfm#contenttop. Implementation of the plans started in 2009-2010. In 2010-2011, the OPC will: • Implement, monitor progress, and continuously report accomplishments against the approved plan to advance each of the four priority privacy issues.
3. Strategically advance global privacy protection for Canadians	Previous	SO 1	Governments and businesses increasingly operate transnationally. The OPC will continue to work with international stakeholders to advance global privacy protection for Canadians. The OPC will: • Develop and sustain partnerships with data protection authorities, international associations and selected regulators. • Selectively intervene with global organizations that may be considering the introduction to Canada of new practices and technologies with significant privacy impact to enhance their awareness and improve compliance.
4. Support Canadians, organizations and institutions to make informed privacy choices	Previous	SO 1	The OPC will continue to provide Canadians with information and tools to understand and protect their privacy rights. The Office will also work with organizations and institutions to understand their privacy obligations and comply with applicable legislation. The OPC will: • Continue to identify emerging privacy risks. • Develop and deliver a broader range of guidance through mechanisms such as inquiries, investigations, PIA reviews, audits, public education, parliamentary appearances and media outreach. • Enhance awareness of key privacy issues among targeted audiences.

[2] "Type" is defined as **previous** (committed to in the first or second fiscal year prior to this RPP); **ongoing** (committed to at least three fiscal years prior to this RPP), or **new** (committed to in this RPP).

Corporate Priority	Type[2]	Link to Strategic Outcome	Description
5. Enhance and sustain organizational capacity	Ongoing	SO 1	Over the past five years, the organization has more than doubled in size and budget to meet a constantly growing demand for privacy protection. More than ever, the OPC relies on its competent and dedicated staff, and understands that they, in turn, require a work environment that is conducive to performance through access to information and state-of-the-art tools. In 2010-2011, the OPC will: • Continue to employ innovative human resources management approaches, including knowledge acquisition and growth, to support a healthy organization and service-delivery improvements. • Develop and use tools, including technology, to better integrate work processes, methods and data, and to foster synergies between OPC branches in order to increase knowledge and information sharing. • Develop a long-term accommodation strategy.

Risk Analysis

External factors and key risks influence the OPC's choice of corporate priorities, affect plans and performance, and drive decision-making. The OPC continually scans its environment to remain responsive to change. This section describes the strategic context for the priority activities presented in the preceding table.

External Factors

A large proportion of Canadians have access to high-speed telecommunications networks and spend a significant amount of time communicating with one another, taking advantage of online services, and participating in online communities. Networked technology strengthens existing relationships and promotes bonds among individuals with similar interests.

In step with this trend, governments and private-sector organizations are also increasingly likely to move their operations online. That, in turn, tends to lead to the collection of extensive amounts of personal information.

The preferences and purchasing intentions of Canadian consumers are valued by advertisers and merchants. The capacity for organizations to direct targeted advertising at individuals will only increase as mobile devices become more common, especially if they emit data on their geographic location.

Personal information is of paramount interest to national security and law enforcement agencies as well. In fact, telecommunications service providers may soon be directed to build infrastructure that can capture significant quantities of data and make it available to law enforcement agencies. This would allow agencies to pursue leads, conduct surveillance, launch investigations, and share data with international law enforcement and national security partners.

Many citizens, for their part, appear willing to exchange their personal information for relatively little reward. Individuals today are exchanging personal information with a mounting number of other people

and organizations, in both the private and public sectors, at home and abroad. Indeed, it is now possible to become the "friend" of a corporate marketing mascot and the "fan" of a brand of detergent.

Privacy regulators around the world struggle with the enforcement of privacy rights and data protection legislation in this new environment. What is the appropriate level of intervention in this situation? What do Canadians expect from privacy regulators?

The OPC's challenge is to find an approach that promotes technological innovation, while ensuring that Canadians' privacy rights continue to be protected. In practice, this will involve a combination of public education, guidance and, where necessary, investigative action and sometimes litigation. Given the pervasive nature of these new technologies, the Office will continue to work with international counterparts to address the privacy challenges created by this new reality.

Key Risks

For the OPC to be successful in this environment, it must manage risks to its activities through controls and mitigating strategies. While risks are managed every day, the Office formally updates its corporate risk profile once a year to document its risk actions, including categorizing risks based on their likelihood and severity of potential impact. Here are the three most critical risks currently faced by the Office:

1. Business Demand

Business demands continue to exceed the capacity of the organization. As such, the Office could find itself unable to meet all of its legislative and mandated requirements, or failing to deliver on a public commitment. The Office has, however, taken a number of steps to address the challenge:

- Over the past few years, the OPC has invested substantial effort to reduce a backlog of investigations and Privacy Impact Assessment (PIA) reviews, and to streamline work processes through a major re-engineering project. The Office will continue to explore the use of alternative interventions to respond to demands more efficiently.

- Since 2005-2006, the OPC has secured additional funding, which was used to increase capacity and to meet new responsibilities, such as expanded public outreach activities and the delivery of programs in the context of the *Federal Accountability Act*.

- As privacy issues proliferate, the Office has become more strategic by tackling four key emerging issues as priorities. They are: information technology, national security, identity integrity and protection, and genetic information.

- The OPC will continue to employ diverse staffing and contractual strategies to build and maintain the necessary organizational capacity, while constantly monitoring resource levels.

These actions have mitigated this capacity risk but the OPC remains vulnerable as demands continue to increase and the specialized investigative and audit skills needed by the Office remain in short supply in the labour market. For now, however, the OPC remains on track in implementing its resourcing strategy from the 2008-2011 Integrated Business and Human Resources Plan.

2. Data Protection

Protecting data from unauthorized disclosure is a second key challenge for the OPC.

The OPC already has significant security measures and safeguards in place. For example, it conducts periodic threat and risk assessments, uses encrypted USB storage devices and web filtering, registers all visitors at reception, and provides regular information-security training to staff.

In February 2009, the OPC also implemented a new privacy breach policy. As an added measure, an internal audit of information security is currently underway, with the resulting recommendations expected to be implemented during the 2011-2012 fiscal year.

Even so, data may be vulnerable to breach, either through system or human error. Risks include the inadequate or inconsistent application of internal security procedures, improper system architecture, or roles-based access to systems, a term used in informatics to indicate that an employee's access to an organization's information system is based on his or her role.

As with any organization, the modern reliance on technological tools to manage operations and exchange information demands that internal security procedures be scrupulously applied.

3. Investigations Backlog

The third critical risk to the OPC is the possibility of not completing the elimination of the investigations backlog by March 2010, as originally planned. The backlog consists of all complaints files that are older than one year, from the time of receipt by the Office.

The OPC has been treating the backlog issue as its first priority for several years. In 2008-2009, the OPC obtained additional funding from Treasury Board for several initiatives, including the elimination of the backlog within a clearly stated deadline.

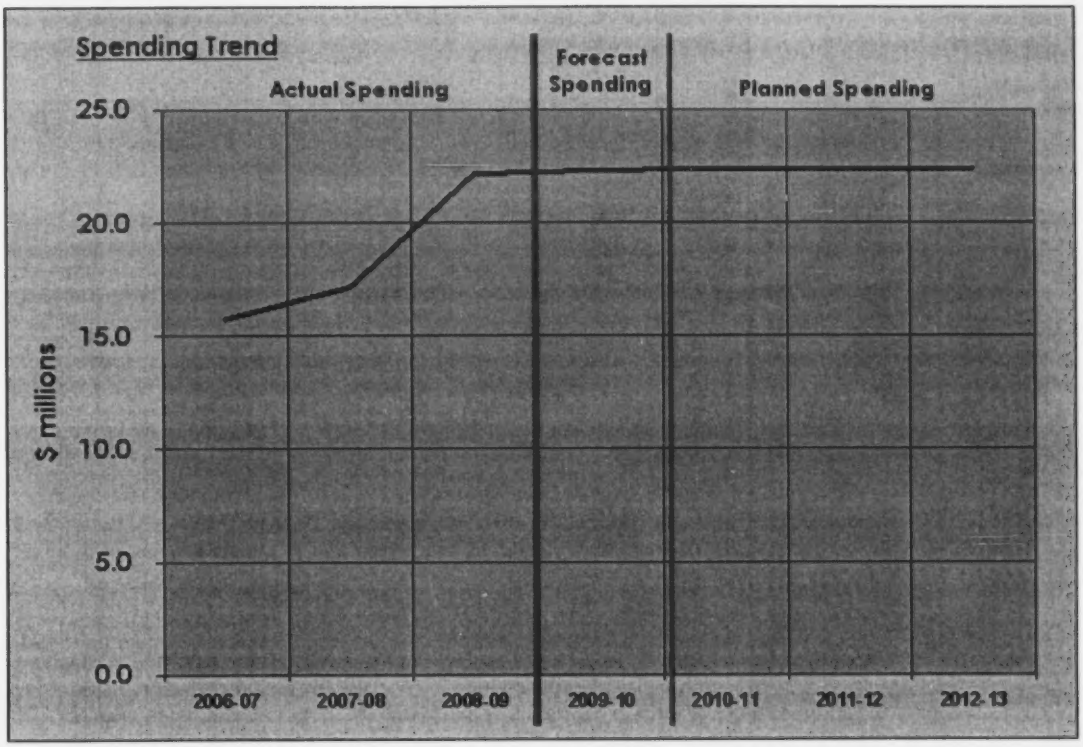
At the time of preparing this report, the backlog had been reduced from 725 files in November 2008 to 283 files in December 2009, and additional measures were being implemented to eliminate it completely. However, the risk remains as well as a few complex cases, which are difficult to quantify at this time, may not be closed by the end of the fiscal year.

Expenditure Profile

In 2010-2011, the OPC plans to spend $22.39 million to advance its five corporate priorities, meet the expected results of its Program Activities, and contribute to its Strategic Outcome.

Spending Trend from 2006-2007 to 2012-2013

The figure below illustrates the OPC's spending trend over a seven-year period.



The graph shows a steady increase in reference-level resources for the period 2006-2007 through to 2009-2010, then a fixed state from 2010-2011 onward. The increased spending reflects resources sought by the OPC through two business cases, as submitted to the *Parliamentary Panel on the Funding and Oversight of Officers of Parliament*.

In 2005, the OPC received increased funding to oversee the implementation of PIPEDA, and in support of its overall mandate. In 2008, the Office also received increased funding to:

- deliver programs in light of new legislation such as the *Federal Accountability Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*;
- eliminate the backlog of privacy investigations;
- expand public outreach, and
- establish an internal audit function.

The funding increase has been phased in over three fiscal years, 2008-2009, 2009-2010 and 2010-2011. The increase for 2008-2009 was $3.3M and for 2009-2010 it is $1.2M. In 2010-2011 and future years, the sunset provision for the funding ($0.4M) earmarked for the backlog elimination is offset by the resources received to compensate for collective bargaining.

2010-2011 Allocation of Funding by Program Activity

The figure below displays the allocation of the OPC's funding by program activity for 2010-2011. More than four-tenths of the funds are allocated to Program Activity 1, Compliance Activities, which includes the Office's main program delivery mechanisms – complaint investigations, responses to inquiries, audits, and privacy impact assessment reviews.

The OPC already has significant security measures and safeguards in place. For example, it conducts periodic threat and risk assessments, uses encrypted USB storage devices and web filtering, registers all visitors at reception, and provides regular information-security training to staff.

In February 2009, the OPC also implemented a new privacy breach policy. As an added measure, an internal audit of information security is currently underway, with the resulting recommendations expected to be implemented during the 2011-2012 fiscal year.

Even so, data may be vulnerable to breach, either through system or human error. Risks include the inadequate or inconsistent application of internal security procedures, improper system architecture, or roles-based access to systems, a term used in informatics to indicate that an employee's access to an organization's information system is based on his or her role.

As with any organization, the modern reliance on technological tools to manage operations and exchange information demands that internal security procedures be scrupulously applied.

3. Investigations Backlog

The third critical risk to the OPC is the possibility of not completing the elimination of the investigations backlog by March 2010, as originally planned. The backlog consists of all complaints files that are older than one year, from the time of receipt by the Office.

The OPC has been treating the backlog issue as its first priority for several years. In 2008-2009, the OPC obtained additional funding from Treasury Board for several initiatives, including the elimination of the backlog within a clearly stated deadline.

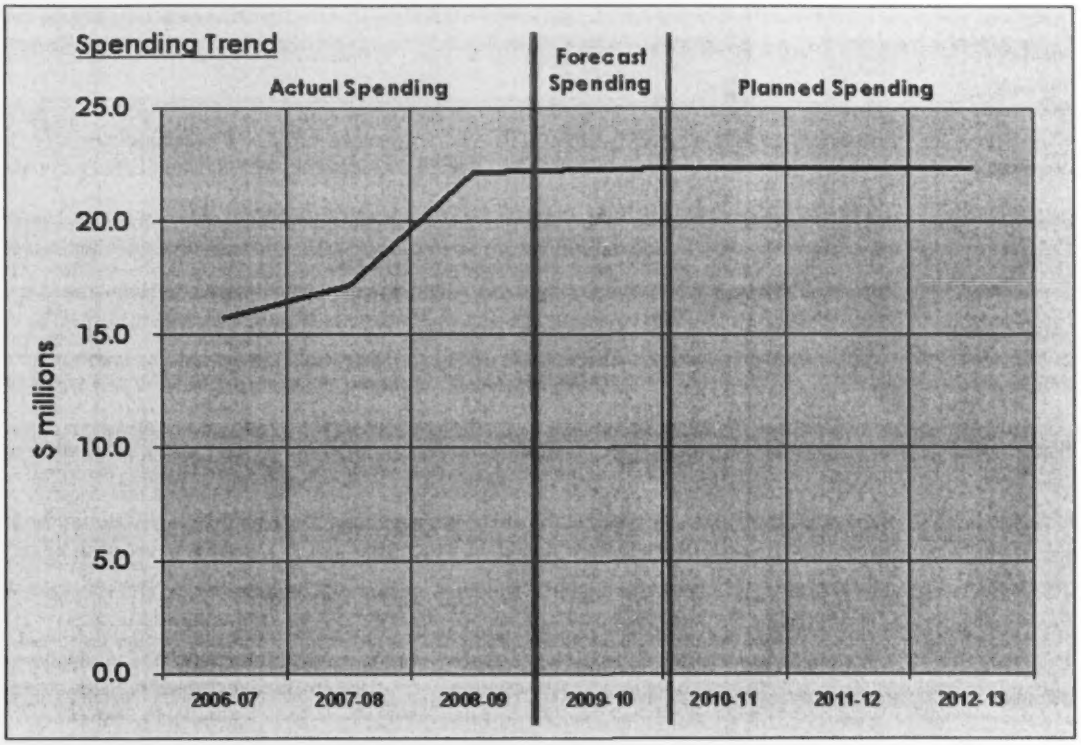
At the time of preparing this report, the backlog had been reduced from 725 files in November 2008 to 283 files in December 2009, and additional measures were being implemented to eliminate it completely. However, the risk remains as well as a few complex cases, which are difficult to quantify at this time, may not be closed by the end of the fiscal year.

Expenditure Profile

In 2010-2011, the OPC plans to spend $22.39 million to advance its five corporate priorities, meet the expected results of its Program Activities, and contribute to its Strategic Outcome.

Spending Trend from 2006-2007 to 2012-2013

The figure below illustrates the OPC's spending trend over a seven-year period.



The graph shows a steady increase in reference-level resources for the period 2006-2007 through to 2009-2010, then a fixed state from 2010-2011 onward. The increased spending reflects resources sought by the OPC through two business cases, as submitted to the *Parliamentary Panel on the Funding and Oversight of Officers of Parliament*.

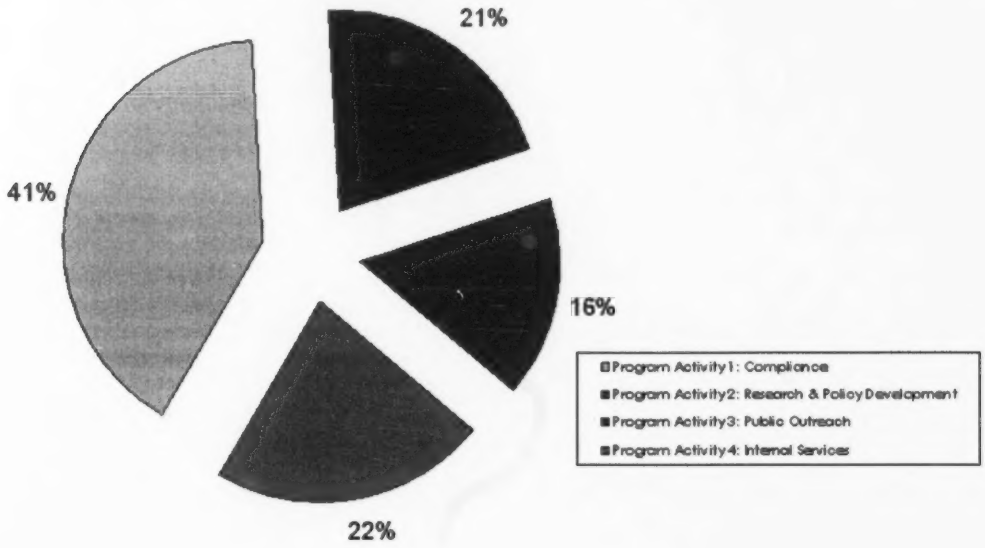
In 2005, the OPC received increased funding to oversee the implementation of PIPEDA, and in support of its overall mandate. In 2008, the Office also received increased funding to:

- deliver programs in light of new legislation such as the *Federal Accountability Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*;
- eliminate the backlog of privacy investigations;
- expand public outreach, and
- establish an internal audit function.

The funding increase has been phased in over three fiscal years, 2008-2009, 2009-2010 and 2010-2011. The increase for 2008-2009 was $3.3M and for 2009-2010 it is $1.2M. In 2010-2011 and future years, the sunset provision for the funding ($0.4M) earmarked for the backlog elimination is offset by the resources received to compensate for collective bargaining.

2010-2011 Allocation of Funding by Program Activity

The figure below displays the allocation of the OPC's funding by program activity for 2010-2011. More than four-tenths of the funds are allocated to Program Activity 1, Compliance Activities, which includes the Office's main program delivery mechanisms – complaint investigations, responses to inquiries, audits, and privacy impact assessment reviews.



Voted and Statutory Items

The Table below illustrates Parliament's approval of OPC resources and shows the changes in resources derived from the supplementary estimates and other authorities, as well as how funds were spent.

Voted and Statutory Items displayed in the Main Estimates

($000)

Vote # or Statutory Item	Truncated Vote or Statutory Wording	2009–2010 Main Estimates	2010–2011 Main Estimates
45	Program expenditures	**20,101**	20,099
(S)	Contributions to employee benefit plans	**2,222**	2,291
	Total	**22,323**	22,390

Section II: Analysis of Program Activities

2.1 Strategic Outcome

All OPC efforts and activities are directed towards achieving the Strategic Outcome, the protection of individuals' privacy rights. The Office plays a leadership role in encouraging organizations that handle Canadians' personal information to respect the privacy rights of individuals. Others who contribute to this mission include provincial and territorial privacy commissioners; international organizations, including data protection authorities; privacy advocacy groups; chief privacy officers; professional associations; consumer representatives; academics; Parliamentary committees, and government departments and agencies.

Strategic Outcome: The privacy rights of individuals are protected.		
Expected Result	**Performance Indicator**	**Target**
Ultimate Outcome for Canadians		
The OPC plays a lead role in influencing federal government institutions and private-sector organizations to respect the privacy rights of individuals and protect their personal information.	Extent and direction of change in the privacy practices of federal government institutions and private-sector organizations.	*Note: Baseline data being developed in 2009-2010 will be used to set a target level for this indicator during 2010-2011. The target will be published in the next RPP.*
Performance Measurement Strategy		
This "umbrella indicator" is based on performance information generated from the following indicators used to measure the OPC Program Activities (PA): • Extent to which investigation recommendations (from 'well-founded', 'resolved' and 'well-founded and resolved' investigations) are accepted and implemented over time (Refer to PA 1); • Extent to which audit recommendations are accepted and implemented over time (Refer to PA 1); • Value added to Parliament of the OPC's views on the privacy implications of relevant laws and regulations (Refer to PA 2); • Value added to stakeholders of the OPC's positions on the privacy implications of relevant policies and initiatives (Refer to PA 2); • Privacy outcome for government initiatives or programs from the PIA consultations/recommendations (Refer to PA 3); • Extent to which private-sector organizations understand their obligations under federal privacy legislation (Refer to PA 3).		

The OPC has four Program Activities and each is presented in the subsections of Section II with the following structure: a description of the Program Activity; a table with information on the expected results for Canadians, the performance indicators and targets as well as the performance measurement strategy to be employed for the measurement; the allocated financial and human resources; the planning highlights with the major activities for 2010-2011, and the benefits for Canadians.

Over the past year, the OPC has revised some performance indicators and targets published in last year's *Report on Plans and Priorities*, in order to generate more useful and reliable performance information for decision-making and reporting. In addition, a few indicators are presented for the first time

in this *Report on Plans and Priorities* as they were introduced in 2009-2010, this being the third year of a three-year implementation of the OPC performance measurement framework first developed in 2007-2008.

The planning highlights for each Program Activity are linked to one or more of the OPC's corporate priorities, as described in the next subsections. The second corporate priority ("Provide leadership to advance issues relating to: information technology, national security, identity integrity and protection, and genetic information") will continue to bring focus to all OPC investigative, audit, research, outreach and other activities. More specifically, in 2010-2011, the OPC will pursue this priority by carrying out and reporting on the following and other activities:

- Expand in-house monitoring and analysis of new technologies based in the public and private sectors, and their impact on the privacy protections of Canadians.
- Continue the development and distribution of tools and activities to help Canadian youth protect their privacy online.
- Acquire a more detailed understanding of how private- and public-sector entities are collecting and using the personal information of Canadians.
- Continue to give priority to Privacy Impact Assessments (PIAs) that have a national security focus. For example, the Office expects to receive PIAs dealing with information sharing among provincial, national and international law enforcement and security agencies.
- Follow-up on the Commissioner's recommendations in the audit of the RCMP exempt databanks (February 2008 – report available at http://www.priv.gc.ca/information/pub/ar-vr/rcmp_080213_e.cfm
- Enhance working relationships with Parliament's national security-related committees and commissions to inform debate, decision-making and recommendations regarding privacy.
- Help organize two workshops to foster dialogue between the research community and federal policy-makers on policy issues arising from the increasing availability of genetic information.
- Continue developing in-house expertise, working towards the preparation of a policy paper on the privacy issues arising from the use of genetic information.

2.2 Program Activity 1: Compliance Activities

Activity Description

The OPC is responsible for investigating privacy-related complaints and responding to inquiries from individuals and organizations. Through audits and reviews, the OPC also assesses how well organizations are complying with requirements set out in the two federal privacy laws, and provides recommendations on Privacy Impact Assessments (PIAs) pursuant to Treasury Board Secretariat policy. This activity is supported by a legal team that provides specialized legal advice and litigation support, and a research team with senior technical and risk-assessment support.

Program Activity 1: Compliance Activities		
Expected Results	**Performance Indicators (Performance Measurement Strategy)**	**Targets**
Intermediate Outcomes		
Federal government institutions and private-sector organizations meet their obligations under federal privacy legislation and implement modern practices of personal information protection.	Extent to which investigation and audit recommendations are accepted and implemented over time (Tracking and analysis of responses to investigation and audit reports)	90% of 'well-founded', 'resolved' and 'well-founded and resolved' investigation recommendations are accepted and implemented 90% of audit recommendations are accepted fully by entities Upon follow-up two years after the initial report, action to implement has begun on 90% of recommendations
	Extent to which obligations are met through litigation (Review and analysis of litigation files and statistics on settlements)	Legal obligations are met in 80% of cases, either through settlements to the satisfaction of the Commissioner or court-enforced judgments
Immediate Outcomes		
Individuals receive timely and effective responses to their inquiries and complaints.	Timeliness of OPC responses to inquiries and complaints (Analysis of Office statistics on turnaround time and backlog status)	*Note: the OPC just completed a major review of its inquiry and complaint investigation processes; service standards are being set and will serve as targets (to be published in the next RPP).*
The privacy practices of federal government institutions (including Privacy Impact Assessments for new and existing government initiatives) and of private-sector organizations are audited and/or reviewed to determine their compliance with federal privacy legislation and policies.	Proportion of audits and PIA reviews completed within planned times (Review and analysis of statistics on audit and PIA project completion)	50% of audits are completed within planned times and 50% of PIA reviews are completed within 90 days of initiation *(targets to be revisited once the OPC reaches full capacity)*
	Responsiveness of (or feedback from) federal government departments and private-sector organizations to OPC advice relating to PIAs and interventions (Tracking and analysis of responses to PIAs and interventions)	75% of institutions and organizations are responsive to OPC advice

Allocated Financial and Human Resources for Program Activity 1

Adjusted Planned Spending	2010-2011	2011-2012	2012-2013
Financial Resources ($000)	9,198	10,152	10,152
Human Resources (FTEs)	88	90	90

Planning Highlights for Program Activity 1

Over the next three years, the OPC will work toward the above Compliance Activities outcomes, while also supporting its first corporate priority – "Redefine service delivery through innovation to maximize results". In 2010-2011, therefore, the OPC will supplement its usual activities with the following initiatives:

- Refine the inquiries and complaints intake function to more accurately assess potential complaints and assign resources proportionately and early in the process.
- Share strategic intelligence about emerging privacy issues and trends with other areas of the Office.
- Increase the number and/or scope of investigations on systemic privacy issues to identify systemic solutions.
- Implement a quality-assurance program for the complaints-resolution process, in order to validate the re-engineering principles applied recently to streamline the process and to provide a vehicle for ongoing service delivery improvement.
- Enhance the strategic planning of audits by basing them on thorough risk analyses and improve the efficiency of the audit function with new standardized audit methodology.
- Conduct audits in the public sector on the use of wireless devices and the disposal of media containing personal information, and an audit of select mortgage brokers in the private-sector.
- Strengthen the Privacy Impact Assessment review process by enhancing the privacy criteria, detailing expectations from federal institutions, offering training to government officials, establishing a repertoire of reviews, and publishing PIA reviews.
- Enforce the legal obligations of organizations through settlements and court-enforced compliance.
- Participate in the creation of a global enforcement network through discussions with international counterparts.
- Continue to work with provincial and territorial counterparts on shared privacy issues. For example, in 2009-2010, the Office helped analyze the privacy impacts of introducing enhanced drivers licences in several provinces, as well as the use of automated licence plate recognition technology in British Columbia. In 2010-2011, the Office will continue to work with the provinces and territories on an as-needed basis, and to interface with provinces with substantially similar privacy legislation to ensure consistent application of the law. There is also the possibility of undertaking a collaborative audit with the Department of Homeland Security in the United States.

Benefits for Canadians from Program Activity 1

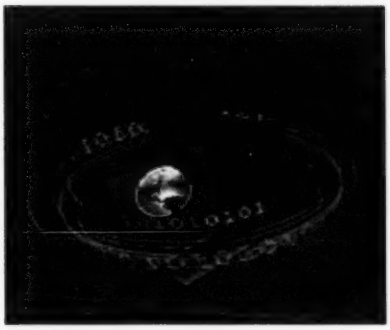
Canadians depend on the investigation services delivered by the OPC to safeguard their privacy rights. Audits and PIA reviews also seek to improve management and accountability for privacy within organizations. OPC recommendations aim to improve organizational systems and practices, thus enhancing the privacy rights of individuals for today and future generations.

And, since privacy has no boundaries, joint and collaborative efforts with provincial/territorial and international counterparts mean more effective enforcement of privacy legislation.

2.3 Program Activity 2: Research and Policy Development

Activity Description

The OPC serves as a centre of expertise on emerging privacy issues in Canada and abroad by researching trends and technological developments, monitoring legislative and regulatory initiatives, providing legal, policy and technical analyses on key issues, and developing policy positions that advance the protection of privacy rights. An important part of the work involves supporting the Commissioner and senior officials in providing advice to Parliament on potential privacy implications of proposed legislation, government programs, and private-sector initiatives.



Expected Results	Performance Indicators (Performance Measurement Strategy)	Targets
Intermediate Outcome		
Parliamentarians and key stakeholders have access to clear, relevant information, and timely and objective advice about the privacy implications of evolving legislation, regulations and policies.	Value added to stakeholders of the OPC information and advice on selected policies and initiatives (Self-assessment of the value-added of the OPC information and advice on key policy files)	75% effectiveness in adding value to the public and private-sector stakeholders through the OPC information and advice on their policies and initiatives
Immediate Outcomes		
The work of Parliamentarians is supported by an effective capacity to identify privacy issues, and to develop privacy-respectful policy positions for the federal public and private sectors.	Value added to Parliament of the OPC views on the privacy implications of relevant laws and regulations (Tracking of support to Parliamentarians, including legislative analysis and appearances at parliamentary committees, through a self-assessment of the value-added of the OPC views)	75% effectiveness in adding value to Parliamentarians from the OPC views on relevant laws and regulations
Knowledge about systemic privacy issues in Canada and abroad is enhanced through information exchange and research, with a view to advancing privacy files of common interest with stakeholders, raise awareness, and improve privacy-management practices.	Stakeholders have had access to, and have considered, the OPC research products and outreach materials in their decision-making (Review of progress reports against the operational plans for the four priority privacy issues to extract evidence that the OPC research products and outreach materials of have had an impact on stakeholders from the OPC research products and outreach materials)	Initiatives under all four (100%) OPC priority privacy issues have involved relevant stakeholders and there is documented evidence demonstrating that they were impacted by the OPC research products and outreach materials

Allocated Financial and Human Resources for Program Activity 2

Adjusted Planned Spending	2010-2011	2011-2012	2012-2013
Financial Resources ($000)	5,058	5,135	5,135
Human Resources (FTEs)	18	19	19

Planning Highlights for Program Activity 2

Over the next three years, the OPC will continue to work towards the above Research and Policy Development outcomes while also supporting its third and fourth corporate priorities ("Strategically advance global privacy protection for Canadians" and "Support Canadians, organizations and institutions to make informed privacy choices"). More specifically in 2010-2011, the OPC will pursue the following initiatives, in addition to its usual activities:

- Continue to act on child privacy, in co-operation and co-ordination with other data protection authorities.
- Conduct consultations on consumer privacy issues with industry, government, consumer associations, civil society and other interested parties on some of the most important emerging issues in privacy – behavioural advertising, cloud computing and location-based data.
- Develop and organize a team of investigators prepared to take on complex investigations in the area of social networking and the use of technology.
- Organize public policy workshops with senior government officials and external experts on emerging privacy issues, with the goal of preparing public policy briefs.
- Explore and communicate the privacy implications of emerging technologies, and whether PIPEDA is able to meet those new challenges.
- Develop and enhance relationships with data protection authorities, international organizations and selected regulators.
- Collaborate with federal partners and international counterparts to implement and enforce the *Electronic Commerce Protection Act*, once it is passed into law.

Benefits for Canadians from Program Activity 2

Knowledge about both emerging and systemic privacy issues is the foundation for OPC advice and guidance, which in turn inform actors about the privacy implications of their actions. For legislators, the implications relate to laws and regulations, and for organizations and Canadians, the implications relate to everyday decisions in the marketplace. An enhanced understanding of national and global privacy issues and a strengthened capacity to address them more effectively are critical for Canada to be recognized as a leader in privacy protection and to positively influence the development of international privacy laws and co-operative agreements.

With the help of effective and well-communicated research activities, policy positions and legal advice from the OPC, decision-makers may better evaluate their actions and measure the privacy risks they assume. Organizations, moreover, are able to comply with their privacy obligations in a more meaningful way.

2.4 Program Activity 3: Public Outreach

Activity Description

The OPC delivers public education and communications activities, including speaking engagements and special events, media relations, and the production and dissemination of promotional and educational material. Through public outreach activities, individuals have access to information about privacy and personal data protection that enable them to protect themselves and exercise their rights. The activities also allow organizations to understand their obligations under federal privacy legislation.

Expected Results	Performance Indicators (Performance Measurement Strategy)	Targets
Intermediate Outcome		
Federal government institutions and private-sector organizations understand their obligations under federal privacy legislations and individuals understand how to guard against threats to their personal information.	Privacy outcome for government initiatives or programs from the PIA consultations/recommendations (Tracking of privacy outcomes from PIA consultations/ recommendations)	In 70% of the government initiatives or programs for which a high priority PIA was reviewed and a recommendation was issued, a privacy protection was added after the consultations/recommendations from the OPC
	Extent to which private-sector organizations understand their obligations under federal privacy legislation (Biennial polling of a sector of private industry)	More than 40% of private-sector organizations report having at least moderate awareness of their obligations under PIPEDA
Immediate Outcomes		

Expected Results	Performance Indicators (Performance Measurement Strategy)	Targets
Individuals have relevant information about their privacy rights and are enabled to guard against threats to their personal information.	Reach of target audience with OPC public education activities. (Analysis of reach based on: media monitoring, hits on the OPC website and blogs, audience size of speeches and events, distribution of materials, etc.)	100 citations of OPC officials on selected communications initiatives per year at least 100,000 hits per month on the OPC website and 20,000 hits per month to the OPC blog at least one news release per month on a subject of particular interest to individuals at least 350 subscribers to the e-newsletter at least 1,000 communication tools distributed per year two public education initiatives annually designed for new individual target groups two public events addressing needs of individual target groups
	Extent to which individuals know about the existence/role of the OPC, understand their privacy rights, and feel they have enough information about threats to privacy (Biennial public opinion polls and other research activities)	at least 20% of Canadians have awareness of the OPC at least 20% of Canadians have an "average" level of understanding of their privacy rights at least 35% of Canadians have some awareness of the privacy threats posed by new technologies
Federal government institutions and private-sector organizations receive useful advice and guidance on privacy rights and obligations, contributing to better understanding and enhanced compliance.	Responsiveness of, or feedback from, federal government departments and private-sector organizations to OPC advice and guidance relating to privacy rights and obligations (Tracking and analysis of the positive and negative feedback/ responses received)	75% of institutions and organizations are responsive to the OPC's advice

Expected Results	Performance Indicators (Performance Measurement Strategy)	Targets
	Reach of organizations with OPC policy positions, promotional activities and promulgation of best practices (Analysis of reach based on: review of Office statistics; analysis of top-10 pages of website and writing of anecdotes on best practices; analysis of targeting, distribution and reach of public education initiatives)	at least 1,000 communication tools distributed per year at least one news release per month on a subject of particular interest to organizations exhibiting at least four times throughout the year at least 350 subscribers to the e-newsletter two public education initiatives annually designed for new organizational target groups two public events/speaking engagements addressing needs of organizational target groups

Allocated Financial and Human Resources for Program Activity 3

Adjusted Planned Spending	2010-2011	2011-2012	2012-2013
Financial Resources ($000)	3,846	3,921	3,921
Human Resources (FTEs)	25	24	24

Planning Highlights for Program Activity 3

Over the next three years, the OPC will continue to work toward the above Public Outreach outcomes while supporting its fourth corporate priority ("Support Canadians, organizations and institutions to make informed privacy choices"). More specifically in 2010-2011, the OPC will pursue the following initiatives in addition to its usual activities:

- Expand outreach and public education activities with industry associations, business development organizations and other stakeholder groups.
- Increase activities under the regional outreach program to speak to more communities across Canada, including partnerships with privacy commissioners in selected provinces and territories.
- Strengthen the review of Privacy Impact Assessments (PIA) and provide an expectations document to federal entities[3] covered under the Privacy Impact Assessment Policy that would offer guidance on what the Office is looking for in PIA reviews. In addition to an assessment of the 10 privacy principles, the intent of the expectations document is to encourage federal entities to demonstrate that:
    - an initiative or program with privacy implications is necessary to achieve a specific purpose;

[3] High-visibility government programs such as the Do-Not-Call List from the Canadian Radio-television and Telecommunications Commission (CRTC), the full-body imaging initiative at airports from the Canadian Air Transport Security Authority (CATSA), and the use of biometrics by Citizenship and Immigration Canada continue to highlight the importance of ensuring that privacy considerations are incorporated into plans when new programs are being developed and implemented.

  - it is likely to be effective in achieving that purpose;
  - the intrusion on privacy is proportional to the benefit to be derived, and
  - no other less privacy intrusive alternative would achieve the same purpose.
- Develop and communicate guidance on privacy for federal public servants, including providing an overview of the *Privacy Act*, reviewing the role of the OPC in reviewing PIAs, highlighting relevant TBS guidelines, and outlining privacy best practices and how they apply in the day-to-day handling of personal information.
- Provide advice and guidance to global organizations to ensure that new technologies and applications comply with PIPEDA.
- Launch and promote the OPC's updated online e-learning tool to help retailers better understand their obligations and comply with PIPEDA, and produce video modules and/or other dynamic tools to help businesses comply with privacy law.

Benefits for Canadians from Program Activity 3

The Privacy Commissioner of Canada has a mandate to raise awareness of rights and obligations under privacy laws. By having a more in-depth understanding of Canadians' views and concerns with respect to their personal information, the OPC is in a better position to educate individuals about their rights, so that they may make informed choices with respect to their personal information protection. As well, by helping organizations understand their responsibilities under federal privacy laws, and by encouraging them to better protect the personal information in their care, Canadians ultimately benefit from enhanced privacy protection.

2.5 Program Activity 4: Internal Services

Activity Description

Internal Services are groups of related activities and resources that support the needs of programs and other corporate obligations of an organization. As a small entity, the OPC's internal services include two sub-activities: governance and management support, and resource management services (which also incorporate asset management services). Given the specific mandate of the OPC, communications services are not included in Internal Services but rather form part of Program Activity 3 – Public Outreach. Similarly, legal services are excluded from Internal Services at OPC, given the legislated requirement to pursue court action under the two federal privacy laws. Legal services form part of Program Activity 1 – Compliance Activities, and Program Activity 2 – Research and Policy Development.

Expected Result	Performance Indicator (Performance Measurement Strategy)	Target
The OPC achieves a standard of organizational excellence, and managers and staff apply sound business management practices.	Ratings against the Management Accountability Framework (MAF) self-assessment (Review of results to the biennial MAF self-assessment exercise and annual progress reports)	Strong or acceptable rating on 70% of MAF areas of management

Allocated Financial and Human Resources for Program Activity 4

Adjusted Planned Spending	2010-2011	2011-2012	2012-2013
Financial Resources ($000)	5,137	5,359	5,359
Human Resources (FTEs)	46	46	46

Planning Highlights for Program Activity 4

The OPC will continue to work toward achieving and maintaining a standard of organizational excellence and have managers and staff apply sound business management practices. Over the next three years, and more particularly in 2010-2011, the OPC will enhance and sustain its organizational capacity (its fifth corporate priority) by pursuing the following Internal Services activities, in addition to its usual activities:

- Continue implementing the OPC Integrated Business and Human Resources Plan 2008-2011, using innovative approaches and solutions to address capacity challenges. These include knowledge acquisition and growth, support for a healthy organization, and service delivery improvements. In 2010-2011, the Plan includes the development of a succession plan for critical positions.
- Foster synergies between OPC branches to increase knowledge and information sharing and to improve decision-making through a variety of new measures in 2010-2011, including:
    - Increasing communication between the inquiries unit and other branches of the Office to provide value-added intelligence about the nature and frequency of inquiries and to develop tools for individuals and organizations;
    - Offering inter-branch and intra-branch developmental assignments to staff and expanding research teams reviewing emerging issues with knowledgeable and interested staff from all branches;
    - Rolling out to all branches an enterprise-wide electronic collaboration tool (SharePoint), which has been successfully piloted in one division of the Office, and providing ongoing training and technical support.

  These new measures complement initiatives already in place and will continue to foster synergies between different areas of the Office. For example, work on the four priority privacy areas identified by the Commissioner (information technology, national security, identity integrity and protection, and genetic information) is led by multidisciplinary teams comprising members from across the Office. There is also a working group that meets twice weekly to discuss issues of interest to various branches, as well as a program of internal and external workshops that examines key challenges to the privacy rights of Canadians.
- Enhance managers' and staff's knowledge and use of information management tools and procedures to maximize capabilities and efficiencies, better support research, policy development and other activities, and improve decision-making. Awareness sessions, group training and individual coaching will be provided in the enterprise-wide electronic documents and records system.
- Evaluate space requirements for the OPC, taking into account present and future needs based on organizational growth. There is, for example, the possibility of an expanded regional presence across Canada. A long-term accommodation strategy to address the renovations to the existing location (Place de Ville in Ottawa) is planned for 2013.

Section III: Supplementary Information

3.1 List of Tables

Table 6 – Internal Audit

The electronic link to the OPC Risk-Based Internal Audit Plan for 2009-2010 to 2011-2012 is: http://www.priv.gc.ca/aboutus/iac/2009/rbap_2009_e.cfm.

Table 11 – Summary of Capital Spending by Program Activity

The following table is located on the Treasury Board Secretariat website:

Program Activity ($000)	Forecast Spending 2009-2010	Planned Spending 2010-2011	Planned Spending 2011-2012	Planned Spending 2012-2013
Internal Services	550	800	550	550
Total	**550**	**800**	**550**	**550**

The increase of $250,000 in 2010-2011 is due to the evergreen replacement of main server infrastructure equipment every three years.

3.2 Other Items of Interest

Legislation Administered by the Privacy Commissioner

Privacy Act	R.S.C. 1985, ch. P21, amended 1997, c.20, s. 55
Personal Information Protection and Electronic Documents Act	2000, c.5

Statutory Annual Reports, other Publications and Information

For further information about the OPC and available resources, please visit the OPC website at http://www.privcom.gc.ca/index_e.cfm or contact the Office at:

Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3
Toll-free: 1-800-282-1376
Phone: (613) 947-1698
Fax: (613) 947-6850
TTY: (613) 992-9190